L Number	Hits	Search Text	DB	Time stamp
1	9132	connectionless proxy	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 08:24
2	398	connectionless and prox$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 08:24
3	32	connectionless same prox$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 08:41
4	6	(connectionless same firewall) and prox$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 08:42
5	51	((connectionless udp icmp ping) same (firewall (fire adj wall))) and prox$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 08:51
6	98	((connectionless udp icmp ping) same (firewall (fire adj wall)))	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:00
7	608	((connectionless udp icmp ping) and (firewall (fire adj wall)))	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:02
8	44	icmp same unreachable	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:05
9	48	icmp same unreachable) (port adj unreachable	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:22
10	77	(key MAC HMAC) and unreachable and (udp icmp connectionless)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:23
13	97	secur$ same connectionless	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:39
15	9	secur$ adj (connectionless udp icmp)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:39
14	367	secur$ same (connectionless udp icmp)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:45
16	136	hmac	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:53
17	7	hmac and firewall	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:46
18	0	hmac same icmp	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:53
20	87	hmac and network	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 10:53

21	60	((connectionless udp icmp ping) and (firewall (fire adj wall))) and (hmac md5)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:03
22	0	(connectionless udp icmp ping) near (hmac md5)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:03
23	0	(connectionless udp icmp ping) near4 (hmac md5)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:03
24	20202	(connectionless udp icmp ping) same4 (hmac md5)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:03
25	19450	(connectionless udp icmp ping) same4 (hmac)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:04
26	6978	(connectionless udp icmp) same4 (hmac)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:04
27	1854	((connectionless udp icmp) same4 (hmac)) and secur$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:05
28	15	((connectionless udp icmp) and (hmac)) and secur$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:14
29	3	(icmp) and (hmac) and secur$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:16
30	370	(icmp) and secur$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:33
31	42	(icmp) same authen$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 11:44
32	95	713/161.ccls.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 12:47
33	204	authen$ same (unreachable unavailable inaccessible)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 12:48
34	139	authen$ same (unreachable unavailable inaccessible) and network	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 13:05
35	3	(authen$ same (unreachable unavailable inaccessible) and network) and ICMP	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 12:49
36	1	(authen$ adj fail$) same (unreachable unavailable inaccessible) and network	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 13:06
37	1	(authen$ adj fail$) same (unreachable unavailable inaccessible)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 13:06
38	203	((authen$ pass$) same fail$) same (unreachable unavailable inaccessible)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 13:07

39	113	((authen$ pass$) same fail$) same (unreachable unavailable inaccessible) and network	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 13:55
51	793	((authen$ pass$) same fail$) same filter and network	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 13:55
52	12	((authen$ pass$) same fail$) same filter and network and 713/201.ccls.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/23 13:56
53	24	(US-6584503-$ or US-6473793-$ or US-6463447-$ or US-6324564-$ or US-6167450-$ or US-6115384-$ or US-6085243-$ or US-6614803-$ or US-6332195-$ or US-6219707-$ or US-5541911-$ or US-5898830-$ or US-6052788-$ or US-6081836-$ or US-6119167-$ or US-6137799-$ or US-6195366-$ or US-6243753-$ or US-5619645-$ or US-6061334-$ or US-6470027-$ or US-6628653-$ or US-4941089-$).did. or (JP-11168511-$).did.	USPAT; JPO	2003/12/23 15:25
54	4	((US-6584503-$ or US-6473793-$ or US-6463447-$ or US-6324564-$ or US-6167450-$ or US-6115384-$ or US-6085243-$ or US-6614803-$ or US-6332195-$ or US-6219707-$ or US-5541911-$ or US-5898830-$ or US-6052788-$ or US-6081836-$ or US-6119167-$ or US-6137799-$ or US-6195366-$ or US-6243753-$ or US-5619645-$ or US-6061334-$ or US-6470027-$ or US-6628653-$ or US-4941089-$).did. or (JP-11168511-$).did.) and unreachable	USPAT	2003/12/23 15:58
55	2016	(packet same key) and @ad<19980604	USPAT; EPO; JPO; DERWENT	2003/12/23 16:01
56	196	(packet same key) and (connectionless udp) and @ad<19980604	USPAT; EPO; JPO; DERWENT	2003/12/23 16:06
57	55	(packet same key) and (connectionless udp) and @ad<19990730 and icmp	USPAT; EPO; JPO; DERWENT	2003/12/23 16:23
58	16	(packet same key) and unreachable and @ad<19990830	USPAT; EPO; JPO; DERWENT	2003/12/23 16:24

Google

Advanced Search Preferences Language Tools Search Tips

hmac rfc Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **hmac rfc**. Results **1** - **10** of about **30,500**. Search took **0.19** seconds.

Category: Computers > Security > Virtual Private Networks > Protocols

HMAC rfc draft (long)
... Index][Thread Index] **HMAC rfc** draft (long). To: ipsec@TIS.COM; Subject: **HMAC rfc** draft (long); From: "H.Krawczyk" <hugo@watson.ibm.com>; ...
www.sandelman.ottawa.on.ca/ipsec/1996/10/msg00058.html - 26k - Cached - Similar pages

Network Working Group H. Krawczyk Request for Comments: 2104 IBM ...
... Krawczyk, et. al. Informational [Page 1] **RFC** 2104 **HMAC** February 1997 **HMAC** can be used in combination with any iterated cryptographic hash function. ...
www.ietf.org/rfc/rfc2104.txt - 23k - Cached - Similar pages

Network Working Group M. Oehler Request for Comments: 2085 NSA ...
... Oehler & Glenn Standards Track [Page 1] **RFC** 2085 **HMAC**-MD5 February 1997 To provide protection against replay attacks, a Replay Prevention field is included as ...
www.ietf.org/rfc/rfc2085.txt - 14k - Cached - Similar pages
[More results from www.ietf.org]

Network Working Group C. Madson Request for Comments: 2404 Cisco ...
... 1. Introduction This memo specifies the use of SHA-1 [FIPS-180-1] combined with **HMAC** [**RFC**-2104] as a keyed authentication mechanism within the context of the ...
csrc.nist.gov/ipsec/papers/rfc2404-hmacsha.txt - 14k - Cached - Similar pages

RFC 2104 (rfc2104) - **HMAC**: Keyed-Hashing for Message ...
... **RFC** 2104 - **HMAC**: Keyed-Hashing for Message Authentication. Network Working Group H. Krawczyk Request for Comments: 2104 IBM Category ...
Description: **HMAC**: Keyed-Hashing for Message Authentication. H. Krawczyk, M. Bellare, R. Canetti. February 1997.
Category: Computers > Internet > RFCs > 2101 - 2200
www.faqs.org/rfcs/rfc2104.html - 24k - Cached - Similar pages

RFC 2404 (rfc2404) - The Use of **HMAC**-SHA-1-96 within ESP and AH
... **RFC** 2404 - The Use of **HMAC**-SHA-1-96 within ESP and AH. Network ... Previous: **RFC** 2403 - The Use of **HMAC**-MD5-96 within ESP and AH. Next ...
Description: The Use of **HMAC**-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998.
Category: Computers > Internet > RFCs > 2401 - 2500
www.faqs.org/rfcs/rfc2404.html - 16k - Cached - Similar pages
[More results from www.faqs.org]

[PDF] Supported VPN Standards
File Format: PDF/Adobe Acrobat - View as HTML
... The AH protocol (**RFC** 2402) allows for the use of various authentication algorithms; PIX Firewall has implemented the mandatory MD5-**HMAC** (**RFC** 2403) and SHA-**HMAC** ...
www.cisco.com/univercd/cc/td/doc/product/ iaabu/pix/pix_62/config/ipsecstd.pdf - Similar pages

Supported VPN Standards
... **RFC** 2402) allows for the use of various authentication algorithms; PIX Firewall has implemented the mandatory MD5-**HMAC** (**RFC** 2403) and SHA-**HMAC** (**RFC** 2404 ...

Advanced Search Preferences Language Tools Search Tips

authenticate unreachable OR una | Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **authenticate unreachable OR unavailable -2000 -2001 -2002 -2003**. Results **1** - **10** of abo

[DOC] ISA Server fails when SQL server is **unavailable**
File Format: Microsoft Word 2000 - View as HTML
... **unavailable**. ISA server stalls its services if the ODBC data source becomes **unavailable** or when it can□t **authenticate** to the SQL server. ...
www.isatools.org/ODBC_Logging_Fix.doc - Similar pages

Interface Commands (aps-**authenticate** - cut-through)
... Router(config-if)# aps **authenticate** sanjose. Router(config-if)# exit. Router(config ... protect interface in the event that the working circuit becomes **unavailable**): ...
www.cisco.com/univercd/cc/td/doc/product/software/ ios122/122cgcr/finter_r/irfacces.htm - 101k - Cached - Similar pages

Pluggable Non Interactive Authentication Modules.: Administration ...
... If this keyword is absent, PNIAM_FAIL is returned if some data is **unavailable** from the application. These modules provide **authenticate** and change functions. ...
www.msu.ru/pniam/pniam-3.html - 20k - Cached - Similar pages

<html> <head> </head><body><pre><html> <head> &lt ...
... Implemented - H 10.5.3 502 Bad Gateway - H 10.5.4 503 Service **Unavailable** t H ... Location t H 14.31 Max-Forwards - H 14.32 Pragma - H 14.33 Proxy-**Authenticate** t H ...
www.w3.org/Protocols/HTTP/Forum/Reports/Tschalaer2.txt - 6k - Cached - Similar pages

HTTP Header response lines and Return Codes
... After, The Retry-After header field can be used with "502 **Unavailable**" to indicate how long the service is expected to be **unavailable**. WWW-**Authenticate**, Must be ...
www.lysator.liu.se/~jmo/http_appendix.html - 7k - Cached - Similar pages

New York City MichNet Number **Unavailable**
New York City MichNet Number **Unavailable** Until Further Notice. ... able to connect to the remote modem on the NAS, but the user cannot **authenticate** successfully or ...
www.itcom.itd.umich.edu/dialin/announcements/NYC.html - 2k - Cached - Similar pages

Sendmail: 451 relay **unavailable**
... E-mail through their UW server -- error message returned says "451 relay **unavailable**". ... It's possible for a user to **authenticate** with a mail server and send a ...
ist.uwaterloo.ca/security/howto/1998-10-20.html - 11k - Cached - Similar pages

pop3.c -- POP3 protocol methods * * Copyright 1998 by Eric S. ...
... else if ((strstr(bufp,"Service") || strstr(bufp,"service")) && (strstr(bufp,"**unavailable**"))) ok = PS_SERVBUSY ... / if (ctl->server.**authenticate** == A_ANY) { ok ...
www.opensource.apple.com/darwinsource/ 10.2.3/fetchmail-7/fetchmail/pop3.c - 24k - Cached - Similar pages

HTTP Response Headers
... Proxy-**Authenticate** - The Proxy-**Authenticate** response-header field MUST be included as ... header field can be used with a 503 (Service **Unavailable**) response to ...
www.comptechdoc.org/independent/web/ http/reference/httpresponse.html - 7k - Cached - Similar pages

<html> <head> </head><body><pre><html> <head> &lt ...

Google™ Advanced Search Preferences Language Tools Search Tips

authenticate unreachable icmp O | Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **authenticate unreachable icmp OR udp -2000 -2001 -2002 -2003**. Results **1** - **10** of abou

[PDF] Threat Models introduced by Mobile IPv6 and Requirements for ...
File Format: PDF/Adobe Acrobat - View as HTML
... Not specific to MIPv6 CN CN HA HA MN MN Attacker Attacker **ICMP Unreachable ICMP Unreachable** Page 12. ... Requirements D2 – MN SHOULD be able to **authenticate** BR. ...
www.ipv6.or.kr/wg/security/Interim/01-005.pdf - Similar pages

<html> <head> </head><body><pre><html> <head> &lt ...
... h> #include <linux/**icmp**.h&gt ... u_short,int); unsigned nameResolve(char *); int **authenticate**(int,char *); unsigned **unreachable**,target; int c ...
www.niksula.cs.hut.fi/~dforsber/synflood/neptune.c - 13k - Cached - Similar pages

Message Formats and Contents
... The purpose of this message is the **authenticate** the mobile node ... **UDP** fields. ... Van Jacobson compression unavailable; 80 home network **unreachable** (**ICMP** error received ...
www.soberit.hut.fi/tik-76.115/98-99/palautukset/ groups/Dynamics/lu/docs/msg_frmts.html - 24k - Cached - Similar pages

Configuring IP Services
... router returns an **ICMP** Destination **Unreachable** message to ... invalid option, it sends an **ICMP** Parameter Problem ... the DRP Server Agent to **authenticate** DRP queries ...
www.cisco.com/univercd/cc/td/doc/product/software/ ios121/121cgcr/ip_c/ipcprt1/1cdip.htm - 101k - Cached - Similar pages

> Configuring IP Services
> ... router returns an **ICMP** destination **unreachable** message to ... invalid option, it sends an **ICMP** parameter problem ... the DRP Server Agent to **authenticate** DRP queries ...
> www.cisco.com/univercd/cc/td/doc/product/software/ ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm - 101k - Cached - Similar pages
> [More results from www.cisco.com]

ICMP in IPSec
... All other **ICMP** messages intended for E1' MUST be dropped. ... traffic is attempting to reach an **unreachable** peer gateway ... and will not be able to **authenticate**, but a ...
www.sandelman.ottawa.on.ca/ipsec/1999/05/msg00062.html - 18k - Cached - Similar pages

[PDF] Wireless Networks
File Format: PDF/Adobe Acrobat - View as HTML
... **unreachable** (**ICMP** error received) 88 home agent **unreachable** (other **ICMP** error received ... insert by encapsulator for the receiver to **authenticate** the source ...
www.cacs.louisiana.edu/~wu/598/note598-3-1.pdf - Similar pages

[PPT] www.iihe.ac.be/homepages/olivier/telorga/Lesson-8.ppt
File Format: Microsoft Powerpoint 97 - View as HTML
... **ICMP** type = dest **unreachable**. **ICMP** code = host **unreachable**. rtr. ... authentication protocol (peer must **authenticate**). .... checksum. **ICMP** Router Solicitation. reserved. ...
Similar pages

RFC 2075 (rfc2075) - IP Echo Host Service

Advanced Search Preferences Language Tools Search Tips

authenticate unreachable rfc icm| Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **authenticate unreachable rfc icmp OR udp -2000 -2001 -2002 -2003**. Results **1** - **10** of al

RFC 2075 (rfc2075) - IP Echo Host Service
... (The **ICMP** Destination **Unreachable** with code 4 is required for MTU discovery under **RFC**-1191 ... problem (such as requiring sources to **authenticate** themselves before ...
Description: IP Echo Host Service. C. Partridge. January 1997.
Category: Computers > Internet > RFCs > 2001 - 2100
www.faqs.org/rfcs/rfc2075.html - 15k - Cached - Similar pages

RFC 2075 - IP Echo Host Service. C. Partridge.
... (The **ICMP** Destination **Unreachable** with code 4 ... **RFC** 2075 IP Echo Host Service January 1997 Security ... such as requiring sources to **authenticate** themselves before ...
rfc.sunsite.dk/rfc/rfc2075.html - 14k - Cached - Similar pages

Network Working Group C. Partridge Request for Comments: 2075 BBN ...
... (The **ICMP** Destination **Unreachable** with code 4 ... Partridge Experimental [Page 3] **RFC** 2075 IP Echo Host ... such as requiring sources to **authenticate** themselves before ...
www.isi.edu/in-notes/rfc2075.txt - 13k - Cached - Similar pages

RFC2075
... (The **ICMP** Destination **Unreachable** with code 4 is required for MTU discovery under **RFC** 1191 ... problem (such as requiring sources to **authenticate** themselves before ...
www.scit.wlv.ac.uk/rfc/rfc20xx/RFC2075.html - 13k - Cached - Similar pages

Configuring IP Services
... The second router returns an **ICMP** Destination **Unreachable** message to ... Time Stamp, which are defined in **RFC** 791. ... the DRP Server Agent to **authenticate** DRP queries ...
www.cisco.com/univercd/cc/td/doc/product/software/ ios121/121cgcr/ip_c/ipcprt1/1cdip.htm - 101k - Cached - Similar pages

Configuring IP Services
... The second router returns an **ICMP** destination **unreachable** message to ... Time Stamp, which are defined in **RFC** 791. ... the DRP Server Agent to **authenticate** DRP queries ...
www.cisco.com/univercd/cc/td/doc/product/software/ ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm - 101k - Cached - Similar pages
[More results from www.cisco.com]

Zvon - **RFC** 2979 - Firewall Requirements
... applications can use to **authenticate** or authorize ... MUST NOT block incoming **ICMP** Destination **Unreachable** / Fragmentation Needed ... ZVON > **RFC** Repository > **RFC** 2979. ...
www.zvon.org/tmRFC/RFC2979/Output/chapter3.html - 9k - Cached - Similar pages

Zvon - **RFC** 2138 - Operation
... obtained such information, it may choose to **authenticate** using RADIUS ... the event that the primary server is down or **unreachable**. ... ZVON > **RFC** Repository > **RFC** 2138. ...
www.zvon.org/tmRFC/RFC2138/Output/chapter2.html - 15k - Cached - Similar pages
[More results from www.zvon.org]

RFC 2522 - web hosting by Directi
... session-key(s) make validity key **authenticate** make privacy ... has received the **ICMP** message

Advanced Search Preferences Language Tools Search Tips

rfc icmp unreachable Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **rfc icmp unreachable**. Results **1** - **10** of about **30,700**. Search took **0.27** seconds.

RFC 792 (rfc792) - Internet Control Message Protocol
... **RFC** 792 Source Address The address of the gateway or host that composes the **ICMP** message. ... [Page 3] September 1981 **RFC** 792 Destination **Unreachable** Message 0 ...
Description: Internet Control Message Protocol. J. Postel. September 1981.
Category: Computers > Internet > RFCs > 0701 - 0800
www.faqs.org/rfcs/rfc792.html - 32k - Cached - Similar pages

Neohapsis Archives - SecurityFocus Pen-test - RE: **ICMP unreachable ...**
... This means that if an OS followed the **RFC** closely, you can potentially ... èåáø 2001 12:05 To: pen-test securityfocus.com Subject: **ICMP unreachable** question. ...
archives.neohapsis.com/archives/ sf/pentest/2001-10/0181.html - 9k - Cached - Similar pages

Neohapsis Archives - Snort discussion - Re: [Snort-users] SMB **RFC**? ...
... message: ronell null.net: "RE: [Snort-users] Can we interpret the **ICMP unreachable** messages?"; In reply to: Fyodor: "Re: [Snort-users] SMB **RFC**?"; Next in thread ...
archives.neohapsis.com/archives/ snort/2000-11/0211.html - 8k - Cached - Similar pages
[More results from archives.neohapsis.com]

icmp - Network services, **ICMP** # # Created by Kurt Seifried, kurt ...
... is of the form: # **icmp** code, **icmp** code name, type code, type name, type description # # 0 echo 0 echo-reply **RFC** 792 - for echo reply message 3 **unreachable** 0 net ...
www.seifried.org/security/ports/icmp.txt - 6k - Cached - Similar pages

Penetration Testing: RE: **ICMP unreachable** question
... This means that if an OS followed the **RFC** closely, you can ... å 26 àå÷èåáø 2001 12:05 To: pen-test_at_securityfocus.com Subject: **ICMP unreachable** question. ...
seclists.org/lists/pen-test/2001/Oct/0190.html - 15k - Cached - Similar pages

Index of tech-net for September, 1997
... 09/05/1997. Alan Barrett, Re: traceroute termination on **ICMP unreachable**. Dave Huang, Re: ppp problem/question. ... 09/16/1997. Matthias Scheler, NetBSD vs. **RFC** 1241. ...
mail-index.netbsd.org/tech-net/1997/09/ - 6k - Cached - Similar pages

tech-net: Re: traceroute termination on **ICMP unreachable**
... claimed that (some/most) > routers rate-limit **ICMP unreachable** messages, so ... [Is there any **RFC**/Internet Draft proposing rate limiting on **ICMP**?] There is ...
mail-index.netbsd.org/tech-net/1997/09/04/0002.html - 3k - Cached - Similar pages
[More results from mail-index.netbsd.org]

pen-test 2001/10: RE: **ICMP unreachable** question
... This means that if an OS followed the **RFC** closely, you can potentially ... èåáø 2001 12:05 To: pen-test@securityfocus.com Subject: **ICMP unreachable** question I ...
lists.jammed.com/pen-test/2001/10/0178.html - 9k - Cached - Similar pages

ICMP TYPE NUMBERS (last updated 2003-11-06) The Internet Control ...
... for Type of Service 12 Destination Host **Unreachable** for Type of ... [RFC1256] Deering, S., Editor, "**ICMP** Router Discovery Messages", **RFC** 1256, Xerox PARC ...
www.iana.org/assignments/icmp-parameters - 8k - Cached - Similar pages

Start new search Search these results Search entire Web

Search: ☑ IEEE Standards Websites ☑ All IEEE Sites
for documents that
must contain | in the body | the words
icmp unreachable
and
must contain | in the body | the words

and
must not contain | in the body | the words

dated
○ Anytime
○ in the last week
◉ on or after 17 December 1980
and before 30 August 2003
and show
100 results | sorted by relevance | with summaries
search Help Simple Search by Inktomi

Results for: +icmp +unreachable **Document count:** +icmp (262) +unreachable

6 results found, sorted by relevance score using date hide summaries

The Effect of Layer-2 Store-and-Forward Devices on Per-Hop Capacity Estimation
The effect of layer-2 store-and-forward devices on per-hop capacity estimation Ravi S. Prasad Constantinos Dovrolis Bruce A. Mah Georgia Tech. Georgia Tech. ...
http://www.ieee-infocom.org/2003/papers/51_02.PDF - 215.0KB - All IEEE Sites - +icmp: 4, +unreachable: 1

IC Online: On the Wire
An SGM-capable router must perform several processes that are not included in the forwarding paths of today's routers. However, for practical deployment, SGM can be supported in an environment that ...
http://basil.computer.org/internet/v4n3/w3onwire-c.htm - 38.1KB - All IEEE Sites - +icmp: 1, +unreachable: 1

Questions ITU-R 215/8 and ITU-R 140/9
C:\ WINDOWS\ TEMP\ 134EV2. DOC 03.05.99 05.05.99 Source: Doc. 8A-9B/TEMP/36 Subject: Questions ITU-R 215/8 and ITU-R 140/9 Principal Rapporteurs, JRG 8A-9B DRAFT NEW ...
http://grouper.ieee.org/groups/802/16/liaison/itu/134ev2.pdf - 470.9KB - IEEE Standards Websites - +icmp: 1,

Search Results

Search Results for: **[(icmp unreachable)<AND>(meta_published_date <= 09-01-1999)]**
Found **1** of **125,779 searched.**

Search within Results

GO > Advanced Search

> Search Help/Tips

Sort by: Title Publication Publication Date Score Binder

Results 1 - 1 of 1 short listing

1 Using pathchar to estimate Internet link characteristics 77%
Allen B. Downey
ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication August 1999
Volume 29 Issue 4

We evaluate **pathchar**, a tool that infers the characteristics of links along an Internet path (latency, bandwidth, queue delays). Looking at two example paths, we identify circumstances where **pathchar** is likely to succeed, and develop techniques to improve the accuracy of **pathchar**'s estimates and reduce the time it takes to generate them. The most successful of these techniques is a form of adaptive data collection that reduces the number of measurements **pathchar** needs ...

Results 1 - 1 of 1 short listing

Advanced Groups Search Preferences Groups Help

icmp unreachable hmac | Google Search

Groups

Web · Images · **Groups** · Directory · News ·

Related groups

comp.dcom.sys.cisco
lucky.openbsd.misc

Searched Groups for **icmp unreachable hmac**. Results **1** - **10** of about **100**. Search took **0.23** seconds.

Sorted by relevance Sort by date

PIX - PIX - VPN Client
... dnat crypto ipsec transform-set myset esp-des esp-md5-**hmac** crypto dynamic ... any any echo-reply access-list out-acl permit **icmp** any any **unreachable** access-list ...
comp.dcom.sys.cisco - Oct 1, 2002 by Jimmy Newbie - View Thread (2 articles)

OpenSSH Login Slowness
... cbc **hmac**-md5 none debug1: kex: client->server aes128-cbc **hmac**-md5 none ... but because there is no blackholing, there is an **ICMP** port **unreachable** sent back to ...
lucky.freebsd.questions - Apr 24, 2003 by Raymond T Sundland - View Thread (1 article)

routing site-to-site vpn with pix 515
... 63.76.144.70 time-exceeded access-list 101 permit **icmp** any host 63.76.144.70 **unreachable** access-list ... transform-set strong esp-des esp-sha-**hmac** crypto map ...
comp.dcom.sys.cisco - Jul 3, 2003 by Chad Mahoney - View Thread (2 articles)

Remote Peer is no longer responding - Pix Firewall
... ethernet1 100full interface ethernet2 auto shutdown **icmp** deny any **unreachable** outside **icmp** deny any ... set ESP-3DES-MD5 esp-3des esp-md5-**hmac** crypto ipsec ...
comp.dcom.sys.cisco - Aug 22, 2002 by magnum7@hotmail.com - View Thread (2 articles)

Problem with Router to Router IPSec
... crypto ipsec transform-set trans1 esp-des esp-md5-**hmac** ! ... permit **icmp** any 222.222.222.96 0.0.0.31 net-**unreachable** access-list 101 permit **icmp** any 222.222 ...
comp.dcom.sys.cisco - May 22, 2003 by Mikhael - View Thread (6 articles)

Re: PIX icmp issue
... list 102 permit **icmp** any host 62.15.39.199 **unreachable** access-list 102 permit **icmp** any host 62.15 ... transform-set standard esp-des esp-md5-**hmac** crypto dynamic ...
comp.dcom.sys.cisco - Jan 1, 2003 by Andreas - View Thread (4 articles)

PIX - PIX VPN
... crypto ipsec transform-set myset esp-3des esp-md5-**hmac** crypto dynamic ... any any echo-reply access-list out-acl permit **icmp** any any **unreachable** access-list out ...
comp.dcom.sys.cisco - Nov 18, 2002 by paul tomlinson - View Thread (1 article)

Re: ICMP fragmentation required but DF set problems.
... **unreachable** to prevent a trivial DoS), 2. disregard any other ... the DF bit set will generate the **ICMP** frag needed ... set and store the (only 16 bit) **HMAC**(srcip|dstip ...
muc.lists.bugtraq - Jan 23, 2001 by antirez - View Thread (3 articles)

Google™ [Advanced Search](#) [Preferences](#) [Language Tools](#) [Search Tips](#)

ipsec unreachable rfc | Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **ipsec unreachable rfc**. Results **1** - **10** of about **7,390**. Search took **0.24** seconds.

NETSYS.COM - The Intelligent Hacker's Choice! **IPSEC** Mailing List ...
... lists.tislabs.com; Sender: owner-**ipsec**@lists.tislabs ... the initiator get an ICMP error 'Host **Unreachable**'? From **RFC** 1009 The ICMP Destination **Unreachable** message ...
www.netsys.com/ipsec/2000/msg00692.html - 10k - Cached - Similar pages

Zvon - **RFC** 2401 - ICMP Processing (relevant to **IPsec**)
... This section discusses **IPsec** handling for Path MTU Discovery messages. ... IPv4 (**RFC** 792 std5): - Type = 3 (Destination **Unreachable**) - Code = 4 (Fragmentation ...
www.zvon.org/tmRFC/RFC2401/Output/chapter6.html - 16k - Cached - Similar pages

Zvon - **RFC** 3329 - Examples
ZVON > **RFC** Repository > **RFC** 3329. ... An attacker could spoof "ICMP Port **Unreachable**" message on the ... 2.0 494 Security Agreement Required Security-Server: **ipsec**-ike;q ...
www.zvon.org/tmRFC/RFC3329/Output/chapter4.html - 9k - Cached - Similar pages
[More results from www.zvon.org]

Re: ICMP "Destination **unreachable**" - should it be sent?
... problem, since it's easy to read **RFC** 2401's current ... by thread: Re: ICMP "Destination **unreachable**" - should it ... Next by thread: Connectathon and IKE/**IPsec** interop ...
www.vpnc.org/ietf-ipsec/00.ipsec/msg01658.html - 6k - Cached - Similar pages

ICMP "Destination **unreachable**" - should it be sent?
... Sender: owner-**ipsec**@xxxxxxxxxxxxxxxxx; User-agent: Mutt/1.2 ... ago, I read the ICMPv6 **RFC** (rfc2463) and ... the following message: "Destination **Unreachable** Message Code ...
www.vpnc.org/ietf-ipsec/00.ipsec/msg01631.html - 5k - Cached - Similar pages
[More results from www.vpnc.org]

<html> <head> </head><body><pre>Network Working Group Michael ...
... v4.txt v1.0, September 1998 Expires in six months IPv4 ICMP messages and **IPsec** security gateways ... Destination **Unreachable** Type 3, defined in **RFC**-0792. ...
www.sandelman.ottawa.on.ca/SSW/ietf/ ipsec-icmp-handle-v4-01.txt - 22k - Cached - Similar pages

Re: ICMP "Destination **unreachable**" - should it be sent?
... problem, since it's easy to read **RFC** 2401's current ... Prev by Date: Re: ICMP "Destination **unreachable**" - should it ... Next by Date: **IPSec** test suite; Prev by thread ...
www.sandelman.ottawa.on.ca/ipsec/2000/10/msg00009.html - 6k - Cached - Similar pages
[More results from www.sandelman.ottawa.on.ca]

Network Working Group Michael Richardson mcr@sandelman.ottawa.on ...
... v4-00.txt> v1.0, September 1998 Expires in six months IPv4 ICMP messages and **IPsec** security gateways ... Destination **Unreachable** Type 3, defined in **RFC**-0792 ...
www.ietf.org/proceedings/99jul/I-D/ draft-ietf-ipsec-icmp-handle-v4-00.txt - 22k - Cached - Similar pages

ICMPv6 Info
... and Encryption of ICMP messages; Changes from **RFC** 2463; ... of ICMPv6 on IKE and **IPsec** Policies:Analysis of the ICMPv6 Messages: Destination **Unreachable**; ...
www2.rad.com/networks/h2003/icmpv6/ - 11k - Cached - Similar pages

Network Working Group R. Atkinson
Request for Comments: 1826 Naval Research Laboratory
Category: Standards Track August 1995

IP Authentication Header

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

ABSTRACT

This document describes a mechanism for providing cryptographic authentication for IPv4 and IPv6 datagrams. An Authentication Header (AH) is normally inserted after an IP header and before the other information being authenticated.

1. INTRODUCTION

The Authentication Header is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. For example, use of an asymmetric digital signature algorithm, such as RSA, could provide non-repudiation.

Confidentiality, and protection from traffic analysis are not provided by the Authentication Header. Users desiring confidentiality should consider using the IP Encapsulating Security Protocol (ESP) either in lieu of or in conjunction with the Authentication Header [Atk95b]. This document assumes the reader has previously read the related IP Security Architecture document which defines the overall security architecture for IP and provides important background information for this specification [Atk95a].

1.1 Overview

The IP Authentication Header seeks to provide security by adding authentication information to an IP datagram. This authentication information is calculated using all of the fields in the IP datagram (including not only the IP Header but also other headers and the user data) which do not change in transit. Fields or options which need to change in transit (e.g., "hop count", "time to live", "ident",

"fragment offset", or "routing pointer") are considered to be zero for the calculation of the authentication data. This provides significantly more security than is currently present in IPv4 and might be sufficient for the needs of many users.

Use of this specification will increase the IP protocol processing costs in participating end systems and will also increase the communications latency. The increased latency is primarily due to the calculation of the authentication data by the sender and the calculation and comparison of the authentication data by the receiver for each IP datagram containing an Authentication Header. The impact will vary with authentication algorithm used and other factors.

In order for the Authentication Header to work properly without changing the entire Internet infrastructure, the authentication data is carried in its own payload. Systems that aren't participating in the authentication MAY ignore the Authentication Data. When used with IPv6, the Authentication Header is normally placed after the Fragmentation and End-to-End headers and before the ESP and transport-layer headers. The information in the other IP headers is used to route the datagram from origin to destination. When used with IPv4, the Authentication Header immediately follows an IPv4 header.

If a symmetric authentication algorithm is used and intermediate authentication is desired, then the nodes performing such intermediate authentication would need to be provided with the appropriate keys. Possession of those keys would permit any one of those systems to forge traffic claiming to be from the legitimate sender to the legitimate receiver or to modify the contents of otherwise legitimate traffic. In some environments such intermediate authentication might be desirable [BCCH94]. If an asymmetric authentication algorithm is used and the routers are aware of the appropriate public keys and authentication algorithm, then the routers possessing the authentication public key could authenticate the traffic being handled without being able to forge or modify otherwise legitimate traffic. Also, Path MTU Discovery MUST be used when intermediate authentication of the Authentication Header is desired and IPv4 is in use because with this method it is not possible to authenticate a fragment of a packet [MD90] [Kno93].

1.2 Requirements Terminology

In this document, the words that are used to define the significance of each particular requirement are usually capitalised. These words are:

- MUST

  This word or the adjective "REQUIRED" means that the item is an absolute requirement of the specification.

- SHOULD

  This word or the adjective "RECOMMENDED" means that there might exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before taking a different course.

- MAY

  This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor might choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2. KEY MANAGEMENT

Key management is an important part of the IP security architecture. However, it is not integrated with this specification because of a long history in the public literature of subtle flaws in key management algorithms and protocols. The IP Authentication Header tries to decouple the key management mechanisms from the security protocol mechanisms. The only coupling between the key management protocol and the security protocol is with the Security Parameters Index (SPI), which is described in more detail below. This decoupling permits several different key management mechanisms to be used. More importantly, it permits the key management protocol to be changed or corrected without unduly impacting the security protocol implementations.

The key management mechanism is used to negotiate a number of parameters for each "Security Association", including not only the keys but also other information (e.g., the authentication algorithm and mode) used by the communicating parties. The key management mechanism creates and maintains a logical table containing the several parameters for each current security association. An implementation of the IP Authentication Header will need to read that

logical table of security parameters to determine how to process each datagram containing an Authentication Header (e.g., to determine which algorithm/mode and key to use in authentication).

Security Associations are unidirectional. A bidirectional communications session will normally have one Security Association in each direction. For example, when a TCP session exists between two systems A and B, there will normally be one Security Association from A to B and a separate second Security Assocation from B to A. The receiver assigns the SPI value to the the Security Association with that sender. The other parameters of the Security Association are determined in a manner specified by the key management mechanism. Section 4 of this document describes in detail the process of selecting a Security Association for an outgoing packet and identifying the Security Assocation for an incoming packet.

The IP Security Architecture document describes key management in detail. It includes specification of the key management requirements for this protocol, and is incorporated here by reference [Atk95a].

3. AUTHENTICATION HEADER SYNTAX

The Authentication Header (AH) may appear after any other headers which are examined at each hop, and before any other headers which are not examined at an intermediate hop. The IPv4 or IPv6 header immediately preceding the Authentication Header will contain the value 51 in its Next Header (or Protocol) field [STD-2].

Example high-level diagrams of IP datagrams with the Authentication Header follow.

```
+------------+------------------+-----------+-------+---------------+
| IPv6 Header| Hop-by-Hop/Routing| Auth Header| Others| Upper Protocol|
+------------+------------------+-----------+-------+---------------+
```

Figure 1: IPv6 Example

When used with IPv6, the Authentication Header normally appears after the IPv6 Hop-by-Hop Header and before the IPv6 Destination Options.

```
+-------------+-------------+-----------------------------+
| IPv4 Header |  Auth Header | Upper Protocol (e.g. TCP, UDP)|
+-------------+-------------+-----------------------------+
```

Figure 2: IPv4 Example

When used with IPv4, the Authentication Header normally follows the main IPv4 header.

3.1 Authentication Header Syntax

The authentication data is the output of the authentication algorithm calculated over the the entire IP datagram as described in more detail later in this document. The authentication calculation must treat the Authentication Data field itself and all fields that are normally modified in transit (e.g., TTL or Hop Limit) as if those fields contained all zeros. All other Authentication Header fields are included in the authentication calculation normally.

The IP Authentication Header has the following syntax:

```
+---------------+---------------+---------------+---------------+
| Next Header   | Length        |           RESERVED            |
+---------------+---------------+---------------+---------------+
|                   Security Parameters Index                   |
+---------------+---------------+---------------+---------------+
|                                                               |
+     Authentication Data (variable number of 32-bit words)     |
|                                                               |
+---------------+---------------+---------------+---------------+
 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8
```

Figure 3: Authentication Header syntax

3.2 Fields of the Authentication Header

NEXT HEADER
8 bits wide. Identifies the next payload after the Authentication Payload. This values in this field are the set of IP Protocol Numbers as defined in the most recent RFC from the Internet Assigned Numbers Authority (IANA) describing "Assigned Numbers" [STD-2].

PAYLOAD LENGTH
8 bits wide. The length of the Authentication Data field in 32-bit words. Minimum value is 0 words, which is only used in the degenerate case of a "null" authentication algorithm.

RESERVED
16 bits wide. Reserved for future use. MUST be set to all zeros when sent. The value is included in the Authentication Data calculation, but is otherwise ignored by the recipient.

SECURITY PARAMETERS INDEX (SPI)
A 32-bit pseudo-random value identifying the security association for this datagram. The Security Parameters Index value 0 is reserved to indicate that "no security association exists".

The set of Security Parameters Index values in the range 1 through 255 are reserved to the Internet Assigned Numbers Authority (IANA) for future use. A reserved SPI value will not normally be assigned by IANA unless the use of that particular assigned SPI value is openly specified in an RFC.

AUTHENTICATION DATA
This length of this field is variable, but is always an integral number of 32-bit words.

Many implementations require padding to other alignments, such as 64-bits, in order to improve performance. All implementations MUST support such padding, which is specified by the Destination on a per SPI basis. The value of the padding field is arbitrarily selected by the sender and is included in the Authentication Data calculation.

An implementation will normally use the combination of Destination Address and SPI to locate the Security Association which specifies the field's size and use. The field retains the same format for all datagrams of any given SPI and Destination Address pair.

The Authentication Data fills the field beginning immediately after the SPI field. If the field is longer than necessary to store the actual authentication data, then the unused bit positions are filled with unspecified, implementation-dependent values.

Refer to each Authentication Transform specification for more information regarding the contents of this field.

3.3 Sensitivity Labeling

As is discussed in greater detail in the IP Security Architecture document, IPv6 will normally use implicit Security Labels rather than the explicit labels that are currently used with IPv4 [Ken91] [Atk95a]. In some situations, users MAY choose to carry explicit labels (for example, IPSO labels as defined by RFC-1108 might be used with IPv4) in addition to using the implicit labels provided by the Authentication Header. Explicit label options could be defined for use with IPv6 (e.g., using the IPv6 end-to-end options header or the IPv6 hop-by-hop options header). Implementations MAY support explicit labels in addition to implicit labels, but implementations are not required to support explicit labels. If explicit labels are in use, then the explicit label MUST be included in the authentication calculation.

4. CALCULATION OF THE AUTHENTICATION DATA

The authentication data carried by the IP Authentication Header is usually calculated using a message digest algorithm (for example, MD5) either encrypting that message digest or keying the message digest directly [Riv92]. Only algorithms that are believed to be cryptographically strong one-way functions should be used with the IP Authentication Header.

Because conventional checksums (e.g., CRC-16) are not cryptographically strong, they MUST NOT be used with the Authentication Header.

When processing an outgoing IP packet for Authentication, the first step is for the sending system to locate the appropriate Security Association. All Security Associations are unidirectional. The selection of the appropriate Security Association for an outgoing IP packet is based at least upon the sending userid and the Destination Address. When host-oriented keying is in use, all sending userids will share the same Security Association to a given destination. When user-oriented keying is in use, then different users or possibly even different applications of the same user might use different Security Associations. The Security Association selected will

indicate which algorithm, algorithm mode, key, and other security properties apply to the outgoing packet.

Fields which NECESSARILY are modified during transit from the sender to the receiver (e.g., TTL and HEADER CHECKSUM for IPv4 or Hop Limit for IPv6) and whose value at the receiver are not known with certainty by the sender are included in the authentication data calculation but are processed specially. For these fields which are modified during transit, the value carried in the IP packet is replaced by the value zero for the purpose of the authentication calculation. By replacing the field's value with zero rather than omitting these fields, alignment is preserved for the authentication calculation.

The sender MUST compute the authentication over the packet as that packet will appear at the receiver. This requirement is placed in order to allow for future IP optional headers which the receiver might not know about but the sender necessarily knows about if it is including such options in the packet. This also permits the authentication of data that will vary in transit but whose value at the final receiver is known with certainty by the sender in advance.

The sender places the calculated message digest algorithm output into the Authentication Data field within the Authentication Header. For purposes of Authentication Data computation, the Authentication Data field is considered to be filled with zeros.

The IPv4 "TIME TO LIVE" and "HEADER CHECKSUM" fields are the only fields in the IPv4 base header that are handled specially for the Authentication Data calculation. Reassembly of fragmented packets occurs PRIOR to processing by the local IP Authentication Header implementation. The "more" bit is of course cleared upon reassembly. Hence, no other fields in the IPv4 header will vary in transit from the perspective of the IP Authentication Header implementation. The "TIME TO LIVE" and "HEADER CHECKSUM" fields of the IPv4 base header MUST be set to all zeros for the Authentication Data calculation. All other IPv4 base header fields are processed normally with their actual contents. Because IPv4 packets are subject to intermediate fragmentation in routers, it is important that the reassembly of IPv4 packets be performed prior to the Authentication Header processing. IPv4 Implementations SHOULD use Path MTU Discovery when the IP Authentication Header is being used [MD90]. For IPv4, not all options are openly specified in a RFC, so it is not possible to enumerate in this document all of the options that might normally be modified during transit. The IP Security Option (IPSO) MUST be included in the Authentication Data calculation whenever that option is present in an IP datagram [Ken91]. If a receiving system does not recognise an IPv4 option that is present in the packet, that option

is included in the Authentication Data calculation. This means that any IPv4 packet containing an IPv4 option that changes during transit in a manner not predictable by the sender and which IPv4 option is unrecognised by the receiver will fail the authentication check and consequently be dropped by the receiver.

The IPv6 "HOP LIMIT" field is the only field in the IPv6 base header that is handled specially for Authentication Data calculation. The value of the HOP LIMIT field is zero for the purpose of Authentication Data calculation. All other fields in the base IPv6 header MUST be included in the Authentication Data calculation using the normal procedures for calculating the Authentication Data. All IPv6 "OPTION TYPE" values contain a bit which MUST be used to determine whether that option data will be included in the Authentication Data calculation. This bit is the third-highest-order bit of the IPv6 OPTION TYPE field. If this bit is set to zero, then the corresponding option is included in the Authentication Data calculation. If this bit is set to one, then the corresponding option is replaced by all zero bits of the same length as the option for the purpose of the Authentication Data calculation. The IPv6 Routing Header "Type 0" will rearrange the address fields within the packet during transit from source to destination. However, this is not a problem because the contents of the packet as it will appear at the receiver are known to the sender and to all intermediate hops. Hence, the IPv6 Routing Header "Type 0" is included in the Authentication Data calculation using the normal procedure.

Upon receipt of a packet containing an IP Authentication Header, the receiver first uses the Destination Address and SPI value to locate the correct Security Association. The receiver then independently verifies that the Authentication Data field and the received data packet are consistent. Again, the Authentication Data field is assumed to be zero for the sole purpose of making the authentication computation. Exactly how this is accomplished is algorithm dependent. If the processing of the authentication algorithm indicates the datagram is valid, then it is accepted. If the algorithm determines that the data and the Authentication Header do not match, then the receiver SHOULD discard the received IP datagram as invalid and MUST record the authentication failure in the system log or audit log. If such a failure occurs, the recorded log data MUST include the SPI value, date/time received, clear-text Sending Address, clear-text Destination Address, and (if it exists) the clear-text Flow ID. The log data MAY also include other information about the failed packet.

5. CONFORMANCE REQUIREMENTS

Implementations that claim conformance or compliance with this specification MUST fully implement the header described here, MUST support manual key distribution for use with this option, MUST comply with all requirements of the "Security Architecture for the Internet Protocol" [Atk95a], and MUST support the use of keyed MD5 as described in the companion document entitled "IP Authentication using Keyed MD5" [MS95]. Implementations MAY also implement other authentication algorithms. Implementors should consult the most recent version of the "IAB Official Standards" RFC for further guidance on the status of this document.

6. SECURITY CONSIDERATIONS

This entire RFC discusses an authentication mechanism for IP. This mechanism is not a panacea to the several security issues in any internetwork, however it does provide a component useful in building a secure internetwork.

Users need to understand that the quality of the security provided by this specification depends completely on the strength of whichever cryptographic algorithm has been implemented, the strength of the key being used, the correctness of that algorithm's implementation, upon the security of the key management mechanism and its implementation, and upon the correctness of the IP Authentication Header and IP implementations in all of the participating systems. If any of these assumptions do not hold, then little or no real security will be provided to the user. Implementors are encouraged to use high assurance methods to develop all of the security relevant parts of their products.

Users interested in confidentiality should consider using the IP Encapsulating Security Payload (ESP) instead of or in conjunction with this specification [Atk95b]. Users seeking protection from traffic analysis might consider the use of appropriate link encryption. Description and specification of link encryption is outside the scope of this note [VK83]. Users interested in combining the IP Authentication Header with the IP Encapsulating Security Payload should consult the IP Encapsulating Security Payload specification for details.

One particular issue is that in some cases a packet which causes an error to be reported back via ICMP might be so large as not to entirely fit within the ICMP message returned. In such cases, it might not be possible for the receiver of the ICMP message to independently authenticate the portion of the returned message. This could mean that the host receiving such an ICMP message would either

trust an unauthenticated ICMP message, which might in turn create some security problem, or not trust and hence not react appropriately to some legitimate ICMP message that should have been reacted to. It is not clear that this issue can be fully resolved in the presence of packets that are the same size as or larger than the minimum IP MTU. Similar complications arise if an encrypted packet causes an ICMP error message to be sent and that packet is truncated.

Active attacks are now widely known to exist in the Internet [CER95]. The presence of active attacks means that unauthenticated source routing, either unidirectional (receive-only) or with replies following the original received source route represents a significant security risk unless all received source routed packets are authenticated using the IP Authentication Header or some other cryptologic mechanism. It is noteworthy that the attacks described in [CER95] include a subset of those described in [Bel89].

The use of IP tunneling with AH creates multiple pairs of endpoints that might perform AH processing. Implementers and administrators should carefully consider the impacts of tunneling on authenticity of the received tunneled packets.

ACKNOWLEDGEMENTS

This document benefited greatly from work done by Bill Simpson, Perry Metzger, and Phil Karn to make general the approach originally defined by the author for SIP, SIPP, and finally IPv6.

The basic concept here is derived in large part from the SNMPv2 Security Protocol work described in [GM93]. Steve Bellovin, Steve Deering, Frank Kastenholz, Dave Mihelcic, and Hilarie Orman provided thoughtful critiques of early versions of this note. Francis Dupont discovered and pointed out the security issue with ICMP in low IP MTU links that is noted just above.

REFERENCES

[Atk95a] Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825, NRL, August 1995.

[Atk95b] Atkinson, R., "IP Encapsulating Security Payload", RFC 1827, NRL, August 1995.

[Bel89] Steven M. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Vol. 19, No. 2, March 1989.

[BCCH94] Braden, R., Clark, D., Crocker, S., and C. Huitema, "Report of IAB Workshop on Security in the Internet Architecture", RFC 1636, USC/Information Sciences Institute, MIT, Trusted Information Systems, INRIA, June 1994, pp. 21-34.

[CER95] Computer Emergency Response Team (CERT), "IP Spoofing Attacks and Hijacked Terminal Connections", CA-95:01, January 1995. Available via anonymous ftp from info.cert.org in /pub/cert_advisories.

[GM93] Galvin J., and K. McCloghrie, "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1446, Trusted Information Systems, Hughes LAN Systems, April 1993.

[Hin94] Bob Hinden (Editor), Internet Protocol version 6 (IPv6) Specification, Work in Progress, October 1994.

[Ken91] Kent, S., "US DoD Security Options for the Internet Protocol", RFC 1108, BBN Communications, November 1991.

[Kno93] Knowles, Stev, "IESG Advice from Experience with Path MTU Discovery", RFC 1435, FTP Software, March 1993.

[MS95] Metzger, P., and W. Simpson, "IP Authentication with Keyed MD5", RFC 1828, Piermont, Daydreamer, August 1995.

[MD90] Mogul, J., and S. Deering, "Path MTU Discovery", RFC 1191, DECWRL, Stanford University, November 1990.

[STD-2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, USC/Information Sciences Institute, October 1994.

[Riv92] Rivest, R., "MD5 Digest Algorithm", RFC 1321, MIT and RSA Data Security, Inc., April 1992.

[VK83] V.L. Voydock & S.T. Kent, "Security Mechanisms in High-level Networks", ACM Computing Surveys, Vol. 15, No. 2, June 1983.

DISCLAIMER

The views and specification here are those of the author and are not necessarily those of his employer. The Naval Research Laboratory has not passed judgement on the merits, if any, of this work. The author and his employer specifically disclaim responsibility for any problems arising from correct or incorrect implementation or use of this specification.

AUTHOR INFORMATION

Randall Atkinson
Information Technology Division
Naval Research Laboratory
Washington, DC 20375-5320
USA

Phone: (202) 767-2389
Fax: (202) 404-8590
EMail: atkinson@itd.nrl.navy.mil